REMARKS

Claims 1-30 remain pending in the present application as amended. Independent claims 1 and 19 have been amended. No claims have been canceled or added. Applicants respectfully submit that no new matter has been added to the application by the Amendment.

The Examiner has rejected claims 1-14, 17-27, 29, and 30 under 35 USC § 102 as being anticipated by Yan et al. (U.S. Patent Pub. No. 2005/0033987). Additionally, the Examiner has rejected claim 15 under 35 USC § 103 as being obvious over the Yan reference in view of Qui (U.S. Patent Pub. No. 2004/0148505), and claims 16 and 28 under 35 USC § 103 as being obvious over the Yan reference in view of Grawrock (U.S. Patent Pub. No. 2004/0117625). Applicants respectfully traverse the Section 102 and 103 rejections.

The present application addresses the situation where two computing entities are to interact and a first one of the entities is required to proffer a showing to the second entity such that the second entity can decide whether to trust the first entity. As part of the proffering, the first entity includes a code ID associated therewith. As is set forth in the specification of the present application at paragraphs 0026-0028, the code ID 16 for a particular first entity 10 is derived or calculated from a digest of the first entity 10 and security information relating thereto such as an id 18, and is typically a hash of same in a manner akin to that which is employed in a digital signature.

The security information in the id 18 specifies security-related aspects of the operation of the first entity 10. In particular, if the first entity 10 wishes to modify its security environment such as for example by reading in a file, opening a debugging port, and the like, the first entity 10 is itself responsible for doing so. However, if a developer developing the first entity 10 wishes to have a particular behavior parameterized, and the parameter has security implications (e.g., open a different file based on program input, or debug based on program input) then the parameter can be placed in the id 18 and the first entity 10 can be written to refer only to the id 18 for the parameter. Thus, although the parameter could potentially be modified within the id 18 by a nefarious entity, the modified id 18 will cause the calculated code ID 16 to change, where such change can be interpreted by an interested party such as the second entity 12 as an indication that the first entity 10 should not be trusted.

In various embodiments, the code ID 16 corresponding to a particular first entity 10 is defined as a hash of the [operating code representative of the] first entity 10 concatenated with the id 18 thereof. The hash may for example be based on any of several known SHA algorithms, including SHA-1 and SHA-256. Accordingly, independent claims 1 and 19 of the present application represent the use of such a code ID to allow a second entity to trust a first entity.

Independent claim 19 recites the use of the code ID from the point of view of the first entity. In particular, in claim 19, the first entity constructs an attestation message to be delivered to the second entity, where the attestation message includes a code identifier (code ID) representative of the first entity and data relevant to the purpose of the trust-based relationship. As now recited, the code ID is publicly available to any entity including the second entity and comprises a one-way hashing function applied to a concatenation of operating code representative of the first entity and security information relating to the first entity but separate from the operating code representative of the first entity. The security information includes at least one security parameter employed by the first entity, and the first entity potentially has multiple versions thereof or employs multiple versions of the security information and thereby potentially has multiple publicly available valid code IDs corresponding thereto. The second entity has knowledge of each valid code ID corresponding to the first entity.

The first entity appends a digital signature to the attestation message and a certificate chain leading back to a trusted root authority, where the signature is based on the code ID and data thereof and is verifiable based on a security key included in the certificate chain. The certificate chain includes at least one certificate therein proffering trustworthiness of the computing device of the first entity, and the first entity sends the attestation message to the second entity and the second entity receives same.

Independent claim 1 recites the use of the code ID from the point of view of the second entity. In particular, in claim 1 the second entity verifies the signature of the received attestation message based on the included security key, whereby alteration of the recited code ID or data of the attestation message should cause the signature to fail to verify and the second entity based on such a failure dishonors such attestation message. The second entity decides whether to in fact enter into the trust-based relationship with the first entity based on

the code ID and the data in the attestation message, where the deciding includes determining that the code ID in the attestation message matches a publicly available code ID for the first entity and known to the second entity. The second entity upon deciding to in fact enter into the trust-based relationship with the first entity constructs a trust message to be delivered to the first entity. The trust message establishes the trust-based relationship and includes therein a secret to be shared between the first and second entities, where such shared secret allows such first and second entities to communicate in a secure manner. The second entity sends the trust message to the first entity and the first entity receiving same, whereby the first entity obtains the shared secret in the trust message and employs the shared secret to exchange information with the second entity according to the established trust-based relationship with such second entity.

As the Examiner notes, the Yan reference discloses at about paragraph 0060 that when an application [first entity] wants to attest its validity to a remote server [second entity], the application sends integrity metrics including C_A, which is a hash of the executable image of the application. Thus, such C_A is akin to the code ID recited in claims 1 and 19. However, and significantly, Yan does not disclose or even appreciate that the application may refer to a security parameter in security information external to the executable image of such application and that the security information could be modified, or that to avoid using such modified security information the security information should or could be included with C_A such that a modification of the security information will cause a calculation of C_A to change, where such change can be interpreted by an interested party as an indication that the application should not be trusted.

As a result, the Yan reference does not disclose or even suggest that C_A is publicly available to any entity including the second entity and comprises a one-way hashing function applied to a concatenation of operating code representative of a first entity [the application] and security information relating to the first entity but separate from the operating code representative of the first entity, as is recited in claims 1 and 19, or that the security information includes at least one security parameter employed by the first entity, and the first entity potentially has multiple versions thereof or employs multiple versions of the security information and thereby potentially has multiple publicly available valid code IDs corresponding thereto, as is also recited in claims 1 and 19, or that the second entity [remote

server] has knowledge of each valid code ID corresponding to the first entity, as is further recited in claims 1 and 19. Likewise, the Yan reference does not disclose or even suggest that the second entity decides whether to in fact enter into a trust-based relationship with the first entity based on such a code ID / C_A and data in an attestation message, where the deciding includes determining that such a code ID / C_A in the attestation message matches a publicly available code ID / C_A for the first entity and known to the second entity, as is moreover recited in claims 1 and 19.

Thus, Applicants respectfully submit that the Yan reference does not anticipate or even make obvious the subject matter recited in claims 1 and 19. Accordingly, Applicants must conclude that such Yan reference cannot be applied to anticipate claims 1 and 19 as amended or any claims depending therefrom, including claims 2-14, 17, 18, 20-27, 29, and 30. Moreover, inasmuch as claims 1 and 19 have been shown to be unanticipated and are non-obvious, then so too must all claims depending therefrom including claims 15, 16, and 28 be unanticipated and non-obvious at least by their dependencies. As a result, Applicants respectfully request reconsideration and withdrawal of the Section 102 and 103 rejections.

In view of the foregoing Amendment and Remarks, Applicants respectfully submit that the present application including claims 1-30 is in condition for allowance and such action is respectfully requested.

Respectfully Submitted,

Date: July 9, 2008

Joseph F. Oriti/
Joseph F. Oriti
Registration No. 47,835

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439